

B. AMENDMENTS TO CLAIMS

Please amend the claims as indicated hereinafter.

1. (CURRENTLY AMENDED) A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to
communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between
the multi-function peripheral device and a user;
one or more processors;
a memory;
a scan process executing in the memory and being configured to cause a printed
document to be scanned at the multi-function peripheral device and to generate
scan data that includes a digital data representation of the electronic document;
a print process executing in the memory and being configured to process print data and
cause a printed version of an electronic document reflected in the print data to be
generated by the multi-function peripheral device at the multi-function peripheral
device; and
a virus protection process executing in the memory and being configured to perform the
steps of: a memory storing instructions which, when processed by one or more
processors, causes the multi-function peripheral to perform the steps of
detecting detect that a request for data to be analyzed for viral infection has been
received by the multi-function peripheral device over the a-network from a
network device; and
in response to detecting receipt of the request, causing the providing data to be
provided from the multi-function peripheral device to the network device
over the network to enable the data to be analyzed for viral infection at the
network device.
2. (ORIGINAL) The multi-function peripheral device as recited in Claim 1, wherein
providing data from the multi-function peripheral device to the network device over the

network includes providing one or more data files to the network device over the network.

3. (ORIGINAL) The multi-function peripheral device as recited in Claim 1, wherein providing data from the multi-function peripheral device to the network device over the network includes providing configuration data to the network device over the network.
4. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the memory stores additional instructions which, when processed by the one or more processors, cause the multi-function peripheral device to perform the steps of: receive replacement data from the network device that has been disinfected; and replace the data on the multi-function peripheral device with the replacement data.
5. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 4, wherein the memory stores other instructions which, when processed by the one or more processors, cause the multi-function peripheral device to after replacing the data on the multi-function peripheral device with the replacement data, generate and send a confirmation message to the network device.
6. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 4, wherein the memory stores other instructions which, when processed by the one or more processors, cause the multi-function peripheral device to, after replacing the data on the multi-function peripheral device with the replacement data, generate a report and either print the report at the multi-function peripheral device or fax the report to another location.
7. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the memory stores additional instructions which, when processed by the one or more processors, cause the multi-function peripheral device to perform the steps of:

receive a request from the network device for the multi-function peripheral device to quarantine or delete at least a portion of the data that was sent from the multi-function peripheral device to the network device; and
in response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the network device.

8. (CURRENTLY AMENDED) A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;
one or more processors;
a memory;
a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of the electronic document;
a print process executing in the memory and being configured to process print data and cause a printed version of an electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and
a virus protection process executing in the memory and being configured to, upon receipt of data by the multi-function peripheral device,
examine the data to determine whether the data contains one or more
unauthorized instructions; and
in response to determining ~~detecting~~ that the data contains one or more
unauthorized instructions, perform one or more actions on the data to protect the multi-function peripheral device.

9. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 8, wherein the virus protection process is further configured to prevent the data from being stored in a non-volatile storage on the multi-function peripheral device.
10. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 8, wherein the virus protection process is further configured to generate and provide a notification that the multi-function peripheral device received the data containing one or more unauthorized instructions.
11. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 8, wherein the one or more unauthorized instructions are unauthorized executable program code.
12. (CURRENTLY AMENDED) A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to
communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between
the multi-function peripheral device and a user;
one or more processors;
a memory;
a scan process executing in the memory and being configured to cause a printed
document to be scanned at the multi-function peripheral device and to generate
scan data that includes a digital data representation of the electronic document;
a print process executing in the memory and being configured to process print data and
cause a printed version of an electronic document reflected in the print data to be
generated by the multi-function peripheral device at the multi-function peripheral
device; and
a virus protection process executing in the memory and being configured to, prior to
sending data from the multi-function peripheral device to a network device over a
network,

examine the data to determine whether the data contains one or more
unauthorized instructions; and
in response to determining that the data contains one or more unauthorized
instructions, perform one or more actions.

13. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 12, wherein the one or more actions include not sending the data to the network device.
14. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 12, wherein the one or more actions include generating and providing a notification that indicates that the multi-function peripheral device has the data that has been infected by a virus.
15. (CURRENTLY AMENDED) The multi-function peripheral device recited in Claim 12, wherein the one or more unauthorized instructions are unauthorized executable program code.
16. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is configured to detect that one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting that the data has been modified.
17. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the data is stored on a non-volatile memory of the multi-function peripheral device.
18. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the data is stored in a volatile memory of the multi-function peripheral device.

19. (ORIGINAL) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.
20. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to determine whether the data stored on the multi-function peripheral device can be restored to a prior state; and in response to determining that the data cannot be restored to the prior state, then delete the data from the multi-function peripheral device.
21. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to render the data inaccessible on the multi-function peripheral device.
22. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to notify a user via the a graphical user interface on the multi-function peripheral device that the data contains one or more unauthorized instructions.
23. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to notify a user by printing a report on the multi-function peripheral device that indicates that the data contains one or more unauthorized instructions.
24. (ORIGINAL) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to provide notification via an email that the data contains one or more unauthorized instructions.

25. (ORIGINAL) The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to provide notification via a facsimile that the data contains one or more unauthorized instructions.
26. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 12, wherein the multi-function peripheral device is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device.